CONTINUATION SHEETS IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

INTRODUCTION AND AGENT BACKGROUND

1. I provide the following in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic cellular telephone device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to the Capital Area Resident Agency office located in York, Pennsylvania. I have been employed as a Special Agent with the FBI since 2021.

3. I am currently assigned to investigate crimes against children including child exploitation and child pornography offenses in violation of Title 18, United States Code, Sections 2252 and 2252A. Additionally, I have been involved with investigations of violations of other federal statutes including fraud, violent crime, online sexual exploitation, and kidnapping. As a Special Agent, one of my primary duties is the enforcement of federal laws and the security of government

witnesses and entities identified during the course of these investigations. I have been trained in conducting financial crime investigations using digital and electronic techniques. I have had the opportunity to review numerous examples of digital evidence and have participated in the execution of many search warrants involving child exploitation offenses.

4. These continuation sheets are intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is a Android One Plus 11 5G cell phone model number CPH2451, hereinafter the "Device". CURRENTLY LOCATED AT **3501 Concord Road, York, PA**

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. FBI Capital Area Resident Agency received information from United States Federal Probation regarding a subject identified as

Dwayne Cavanaugh.

8. Dwayne Cavanaugh is currently a registered sexual offender. According to the Megan's Law database, Cavanaugh's current residential address is 1841 Market Street, Harrisburg, PA. He is currently being supervised on Federal Probation in the Middle District of Pennsylvania and has a previous criminal conviction for possession of child pornography. Cavanaugh plead guilty in 2009 in the Northern District of Texas for receipt of child pornography. He was sentenced to 12 years of imprisonment and a lifetime of supervised release.

9. According to a report receive from United States Probation Officer Joseph Petrarca, Cavanaugh failed a polygraph examination in October 2023. This would have been administered by Commonwealth Clinical Group as directed by a court order to obtain sexual offender treatment.

10. According to Federal Probation Officer John Johnson, Cavanuagh was in a relationship with a female who had partial custody of three young children.

11. Federal Probation Officer John Johnson was conducting a physical surveillance of Cavanaugh while Cavanuagh was visiting his

girlfriend who resides in the Middle District of Pennsylvania. Upon exiting the residence, Probation Officer Johnson made contact with Cavanaugh. Cavanaugh's vehicle was parked at the residence.

12. According to conditions of his supervised release, Cavanaugh is subject to search at any time.

13. On January 21, 2024, a Federal Probation Officer John Johnson participated in a lawful search of Cavanaugh's vehicle. During the course of the search, Probation Officers found an unmonitored cell phone that was stored without a battery. According to the conditions of supervised release, Cavanaugh's electronic devices will be monitored by Federal Probation.

14. According to the report received by USPO Joseph Petrarca, Cavanaugh made admissions to possessing the device and viewing pornography on the device.

15. On January 29, 2024, Federal Probation Officer John Johnson submitted a request to have this electronic device analyzed.

16. Federal Probation Officer Joseph Petrarca conducted an initial forensic examination on this device and completed a report on September 27, 2024. During the course of that initial forensic

examination, it was found that the Google Chrome Browser showed 42 active tabs, all of which contained websites displaying prepubescent child pornography.

17. According to the forensic report completed by USPO Petrarca, the Google Chrome browser data from the device was not able to be captured in the forensic extraction.

18. According to USPO Joseph Petrarca, he viewed the Google Chrome browser images which depicted prepubescent minor females approximately 7-11 years old with their genitals exposed; there was no visible pubic hair on the juveniles.

19. On 11/25/2024, USPO John Johnson conducted a manual review of the device for clarification of what the images depicted. The following was revealed:

a. Upon opening the Google Chrome application there was an option to continue browsing for "Young girls photo and video". All of the visible tabs appeared to have images or titles depicting pornography.

b. A Google Tab with a partial visible title of "Adorable Sho" contained a file which depicted a prepubescent female with

no clothing on from her waist down. There was an unidentified adult male penis pushed against the juvenile's vagina.

c. An additional Google Chrome browser tab had an image which depicted a prepubescent minor female. The image appeared to be zoomed in to focus on the child's vagina. The minor was not wearing any clothing and her genitals were visible. There was no pubic hair present.

d. An additional Google Chrome tab was titled "step daughter". This tab displayed a prepubescent minor female with no clothing on from her waist down. There is an unidentified adult male penetrating the child's genitals with his penis.

20. A search warrant issued in the Middle District of Pennsylvania was obtained for the Nokia cell phone that was previously seized by Federal Probation officers. A manual review of the Nokia cell phone was conducted. The manual search revealed multiple images of illegal child sexual abuse material (CSAM). For example, in the Google browser tabs there was a tab titled "adorable sho" which depicted a prepubescent minor female naked. The child is visible from the waist

down, exposing her genitals. There is an unidentified male penis pushed against the child's vagina. There is an additional tab with the logo "PB" which contained an image of a zoomed in image of a prepubescent minor female's vagina unclothed.

21. On March 5, 2025, Dwayne Cavanaugh was federally indicted for possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5). On 03/06/25, Dwayne Cavanaugh was arrested on charges related to the possession of child pornography. An android cell phone One Plus 11 5G model number CPH2451 was seized incident to his arrest.

22. On the same day as his arrest, Cavanaugh had his initial appearance and arraignment. He was ordered detained pending trial and remained in custody as of the writing of this application.

CHARACTERISTICS COMMON TO CHILD PORNOGRAPHY COLLECTORS

23. I know from my training and experience that the following characteristics are prevalent among individuals who collect child pornography:

a. The majority of individuals who collect child pornography

are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography may collect explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals may also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their sexual fantasies involving children.

c. The majority of individuals who collect child pornography may often seek out like-minded individuals, either in person or via the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet-based vehicles used by such individuals to

communicate with each other include, but are not limited to, peer-to-peer, e-mail, bulletin boards, Internet relay chat, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography may maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often may collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from

which they were derived, in telephone books or notebooks, on computer storage devices, or on scraps of paper.

f. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collection of illicit materials from discovery, theft, and damage. However, some individuals may dispose of their collection of their sexually explicit materials or only seek them out when they want to view them in order to conceal their activities for fear of being caught.

g. Individuals who possess, receive, or produce child pornography often transfer these files between their different online accounts and electronic and storage devices, whether it is to conceal the files, to store them in one account or device versus another account or device, or to use in their communication with other child pornographers. I have investigated cases where individuals transfer child pornography files from one device, or account, or social media application to another. I have investigated cases

where individuals store some or all of their child pornography collections in multiple electronic and storage devices.

DEVICE CONTENT

24. Based on my training and experience, I know that persons involved in criminal activities may use cellular devices to access social media, or other web-based applications. This includes utilizing cellular phones to exchange and access child pornography. In particular, persons involved in criminal activities may use private messaging functions of social media to communicate in furtherance of criminal activities in an effort not to be detected by law enforcement.

25. Based on my training and experience, I know that individuals may use phones to take photographs and videos of themselves and others. Those photographs and videos may show geographic locations, and oftentimes includes metadata showing the date, time and location the image was taken. Cell phones, as well as applications used on cell phones, may contain GPS location data. This information can be used to determine the location of a cell phone, and given the ubiquity of individuals carrying cell phones, is therefore

probative of the location of the owner of the cell phone.

26. The Device is currently in the lawful possession of the Federal Bureau of Investigation (FBI). It came into the FBI's possession in the following way: collected from Dwayne Cavanaugh, incident to arrest. Therefore, while the **FBI** might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that the FBI's examination of the Device will comply with the Fourth Amendment and other applicable laws.

27. The Device is currently in storage at 3501 Concord Road, York, PA. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

TECHNICAL TERMS

28. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless

device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records

pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites

orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data.

e. Internet: The Internet is a global network of computers and

other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

29. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, GPS, and to access the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

30. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

31. There is probable cause to believe that things that were once

stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer/cell phone storage media—in particular, cell phone/computers' internal hard drives—contain electronic evidence of how a computer/cell phone has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer/cell phone users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the

Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Computer/cell phone file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while

executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer or cell phone is evidence may depend on other information stored on the device and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present

on a storage medium.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

34. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

35. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

ATTACHMENT A

Property to Be Searched

1. The property to be searched is an Android One Plus 11 5G cell phone, model number CPH2451, hereinafter the "Device".

CURRENTLY LOCATED AT **3501 Concord Road, York, PA**

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

1. All records and information on the Device described in Attachment A that are evidence, fruits of the crime, or contraband relating to violations of Title 18 U.S.C. § 2252A(a)(2) (Receipt of Child Pornography) including:

   a. All stored electronic and wire communications and information in memory on the target device including email, instant messaging, text messages, other communications, contact lists, images, videos, voice mail, and any other content or records on the device.

   b. Internet search history.

   c. Video clips and photographs digitally stored within the target device's internal memory, SIM card, or other removable data storage device, which constitute evidence of the listed offense, and/or will help agents to identify other persons who are involved in the above listed offense;

   d. Ledgers, receipts, invoices, and other documentary evidence that is stored electronically in the target device's internal

memory, SIM card, or other removable data storage device which constitute evidence of the listed offenses, or which will help agents to identify other persons who are involved in the above listed offense;

e. Evidence of user attribution showing who used or owned the target device at the time the things described in this warrant were accessed, viewed, created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

f. Evidence indicating how and when the Device was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation.

As used above, the terms "communications," "records," and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage (such as SIM card or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and

electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.